ACN*Report*

Fall 2005 Vol. IV, No. 3

A National Security and Emergency Preparedness (NS/EP) Support Program of the National Communications System

Phone Features

Once every year, Alerting and Coordination Network (ACN) administrators like to review with membership the network's voice over Internet protocol (VoIP) telephone capabilities. As 2005 winds down, here is your annual phone feature refresher:

Placing Calls

To call a fellow ACN member, pick up the handset or press the speakerphone button. Dial their four-digit extension.

Voicemail Setup

Press the Voicemail button or dial 3219. Enter the phone extension and press the pound (#) key. An automated prompt requests that you enter your password followed by the pound key. (For specifics on ACN passwords, please refer to the *Password Procedures* section of this article.) After you enter your password, continue following the prompts to record your outgoing message. You should include your organization's name, location and commercial contact number in the outgoing message. Do not use a specific individual's name unless he/she is the only person who will be accessing the mailbox or handling the ACN program at your location.

Sample Outgoing Message: "You have reached [organization's name]. Please leave a detailed message, including your name, organization, ACN phone number, and commercial phone number. We can also be reached at [commercial phone number]. Thank you for calling."

Voicemail Retrieval

When there is a message in the voice mailbox, the message indicator light at the top center of the phone illuminates. To access your ACN voice mailbox and check your messages, press the Voicemail button or dial 3219. Enter your ACN phone extension followed by the pound key. An automated prompt requests that you enter your password followed by

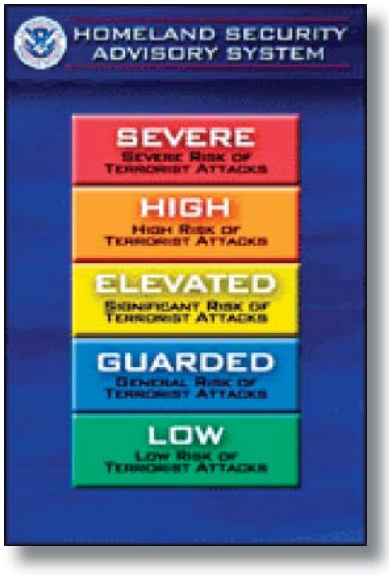
continued on page 2

In This Issue

According To Policy…

ACN and the DHS Threat Advisory System

There understandably has been an increased global focus on reducing the likelihood of further terrorist attacks since the turn of the century. The Department of Homeland Security (DHS) has devised the Homeland Security Advisory System to support this effort. One element of the system, the DHS Color-Coded Threat Level System, uses five different color-coded conditions to communicate the current threat level to the American public. A brief summary of the conditions are provided below, taken from www.dhs.gov:



- LOW Condition (Green): This condition is declared when there is a low risk of terrorist attacks.

continued on page 3

Phone Features *continued from page 1*

the pound key. (For specifics on ACN passwords, please refer to the *Password Procedures* section of this article.) After you enter your password, continue following the prompts to check your messages.

Password Procedures

Press the Voicemail button on the phone or dial extension 3219, enter your assigned extension, and press the pound key. The ACN phone will then prompt you to enter your password. Your default ACN password is your assigned extension listed backwards. For example, if your ACN extension is 4106, then your password is 6014. The exception to this rule is any extension that would be the same both ways, such as 6116. In these cases, replace the first digit of your four-digit extension with a "9." So if your ACN extension is 6116, your default password would be 9116. After you have entered your password, press the pound key.

You are able to change your default password. To change your password, access your voice mailbox and enter options "5" and "4" on the automated menu. Then follow the prompts to change your password.

Help

To contact ACN's 24/7 Help Desk, either press the Help key or dial extension 4357.

Conference Calling

ACN provides two different means of conference calling: the conference feature on the VoIP phone and the ACN conference bridge.

Every ACN member can initiate a conference call via the VoIP phone. The phone accommodates up to six users, including the call originator. To begin a conference call, dial the first user and, after you receive an answer, press the Conference button. To add additional users, simply repeat the preceding steps. Each time you dial a new user and press the Conference button, that user will be added.

Select ACN users have the ability to initiate conference calls via the ACN conference bridge. The ACN Program Manager determines which members require this capability. The conference bridge accommodates up to 115 users at once.

Follow the procedures below to connect to conference bridge calls.

When you answer, wait until the automated voice prompts you to enter your Personal Identification Number (PIN).

- There may be up to a 15-second delay before the prompt.
- There is no audible indicator that you are on hold. Administrators are working to eliminate the delay, but in the meantime, please be advised of this issue and plan accordingly.

Enter your PIN, followed by the pound key. Your PIN is your ACN extension followed by the last two digits of your extension a second time. For instance, extension 5296 has a PIN of 529696#. Officially announce your presence upon joining the call.

A Reliable Backup

The Alerting and Coordination Network (ACN) is the National Communications System's (NCS) contingency plan. It serves as a backup network that can provide stable emergency communications connectivity when the public switched network (PSN) is inoperable, stressed, or congested. ACN facilitates telecommunications service providers' network operations and supports network restoration coordination, transmission of telecommunications requirements and priorities, and incident reporting. When the PSN fails, ACN will be there.

If it sounds too good to be true, it is not. ACN can guarantee reliable backup services, and the reason for that is as follows: every ACN server, conference bridge and private branch exchange (PBX) is redundant. That's right; the backup has its own backup.

Here's a hypothetical scenario. The facility that houses ACN's primary datacenter suffers a major power outage that affects most of the equipment on site. Perhaps one of the circuit breakers fails, causing the uninterruptible power supply (UPS) to rely on battery backup power. The UPS battery eventually discharges, at which time the network fails over to ACN's backup datacenter without missing a beat. The changeover to the backup datacenter is virtually instantaneous and causes no network interruptions. Shortly after the power outage ends, the primary datacenter resumes responsibilities.

In a perfect world, there would be no need for an emergency communications network. Realistically, however, it is nice to know there is something reliable in place. You can feel confident in the knowledge that, during incidents of National significance, the NCS has a solid backup plan: ACN!

Cyber Security

Computers and Beyond

Christopher Leverich
Security Analyst

If you have a personal computer (PC) or laptop at home, by now you are probably aware that there are inherent risks involved. Hackers can break in, viruses can infect, and so forth. Chances are good that you take appropriate countermeasures to mitigate such risks. But while it might be tempting to associate the importance of cyber security exclusively with traditional computers, it would be a mistake to do so.

It's not that the need for cyber security has extended beyond computers. As we journey further into the 21st century, however, the simple truth is that computers are becoming so much more than laptops and PCs. Cell phones, personal digital assistants (PDAs), car navigation systems…all are becoming increasingly vulnerable to cyber attack, because nowadays many electronic devices are connected to computer networks. Any device that incorporates computerized components is vulnerable, especially if it connects to the Internet.

"Any device that incorporates computerized components is vulnerable, especially if it connects to the Internet."

So while it may seem comical to think that an unscrupulous individual could infect your cell phone with a virus, it's already happening. In fact, hackers can now steal your wireless service or highjack information from your PDA.

Consequently, as the devices that have seemingly become a part of everyday life continue to grow more sophisticated, you need to go into defense mode. There are numerous steps you can take to protect yourself. You should make it a habit to keep all patches and software updates current. Doing so can help protect your equipment from known problems or vulnerabilities. You should also make use of any security features that your devices offer. Choose phones and PDAs that allow password protection. If the apparatus has a wireless technology that connects it to other computers, disable this connectivity when not in use. Enable PDA encryption if that is an option. Of course, there is no real substitute for old fashioned physical security. If a hacker cannot get his hands on your equipment, his job becomes immensely tougher.

In the case of the Alerting and Coordination Network (ACN), we have a network that revolves around the voice over Internet protocol (VoIP) phone and is void of laptops or PCs. As I've just illustrated, that alone does not make a safe network. Thanks to industry best security practices, ACN is difficult to penetrate. But it is important that we do not get lulled into a false sense of security simply because our network does not incorporate traditional computers. The fact remains that as the world we live in becomes increasingly wired, wireless and interconnected, more and more of our gadgets will become cyber security concerns. That is the tradeoff for technological advancement. Luckily, with a bit of awareness and know-how, it is a tradeoff that we can mitigate quite effectively.

Mr. Leverich is a Security Analyst for Arrowhead Global Solutions, under contract to the NCS.

Policy *continued from page 1*

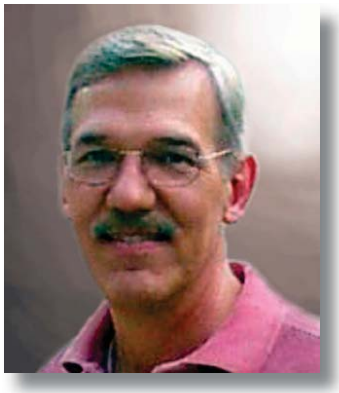
- GUARDED Condition (Blue): This condition is declared when there is a general risk of terrorist attacks.
- ELEVATED Condition (Yellow): An Elevated Condition is declared when there is a significant risk of terrorist attacks.
- HIGH Condition (Orange): A High Condition is declared when there is a high risk of terrorist attacks.
- SEVERE Condition (Red): A Severe Condition reflects a severe risk of terrorist attacks.

How does this tie in with Alerting and Coordination Network (ACN) policy? ACN adheres to the DHS Threat Level System and adjusts network activity accordingly. The current threat advisory condition is ELEVATED (Yellow). As long as the threat level does not rise above ELEVATED, ACN activity continues as normal. If the threat level becomes HIGH or SEVERE, however, ACN administrators may be conducting network communications tests more frequently (presently, administrators conduct one individual line ring-down test and one conference call blast-out test per month). The ACN Program Manager will announce any changes to the frequency of the testing along with specific detailed information pertaining to the threat level.

A "Hazzard" Infiltrates the Network

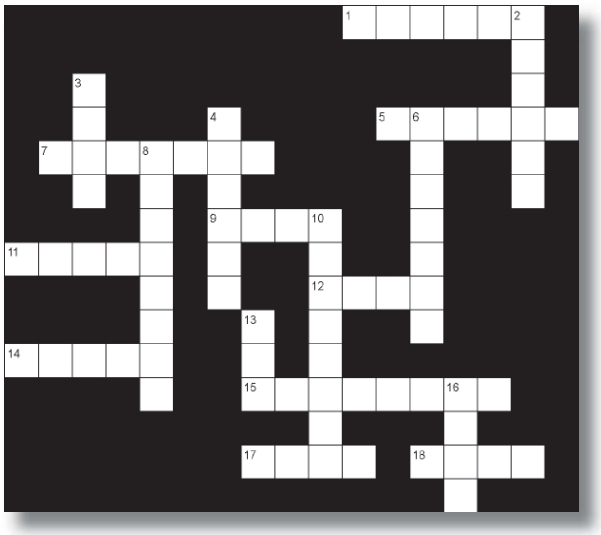
Larry Hazzard is the new Alerting and Coordination (ACN) Task Monitor. No stranger to the regulated telecommunications environment, Mr. Hazzard has extensive experience in both wireless and wire line communications. In a telecommunications career spanning over 30 years, he has worked both in the private sector (Pacific Telephone, Illinois Consolidated Telephone) and the public sector (General Services Administration, Secret Service). Some of his more memorable work experiences include fiber network implementation for the U.S. Patent and Trademark Office and contracting officer technical representative support for the Washington Interagency Telecommunications System.

Mr. Hazzard joined the National Communications System (NCS) this past summer. He noted that ACN is an important element within the NCS and feels the network's importance will continue to rise: "ACN is currently used in support of routine administrative activities and, more significantly, as a backup component for response and recovery actions as appropriate. The value of ACN is likely to increase with today's added emphasis on cyber security support resilience, which I believe is a major strength of the network." Moving forward in his new role, expect Mr. Hazzard to contribute to the ongoing success of ACN.



Mind Bender

Try out an ACN crossword puzzle! You'll find all the words related to the network we know and love. Enjoy!



Across

1. User
5. Not digital
7. Zeros/ones
9. Directorate
11. Dial this
12. Not under
14. Speech instrument
15. Protection (or found in an airport)
17. 4357
18. Nat Sec/Emerg Prep

Down

2. Newsletter
3. Voice over Internet Protocol
4. Protecting our ____
6. AC_
8. www
10. VoI_
13. Dept of Homeland Security
16. ACN Monthly ____

Last Issue's Answer:
THE ACN REPORT
843 226 727678

ACN Program Management Office

Tel: 1-866-NCS-CALL (1-866-627-2255)
1-703-676-CALL (703-676-2255) DC Metro Area
E-mail: acn@dhs.gov
Web: www.ncs.gov/acn

Department of Homeland Security
Information Analysis and Infrastructure Protection Directorate
National Communications System
P.O. Box 4502
Arlington, VA 22204-4502

Technical Support: ACN Help Desk

ACN Ext: 4357 (HELP)
Tel: 1-800-504-4066 (Toll Free)
E-mail: smc@arrowhead.com

24/7 ACN Help Desk:
1-800-504-4066

Monthly Test
1:00-1:30 PM EST
15th of the month,
or the following Monday